Rec'd PCT/PTO 14 APR 2005

10/531616

PCT/IB03/04608
10.11.03

Europäisches Patentamt
European Patent Office
Office européen des brevets

REC'D 19 NOV 2003
WIPO PCT

Bescheinigung Certificate Attestation

Die angehefteten Unterlagen stimmen mit der ursprünglich eingereichten Fassung der auf dem nächsten Blatt bezeichneten europäischen Patentanmeldung überein.

The attached documents are exact copies of the European patent application described on the following page, as originally filed.

Les documents fixés à cette attestation sont conformes à la version initialement déposée de la demande de brevet européen spécifiée à la page suivante.

Patentanmeldung Nr. Patent application No. Demande de brevet n°

02257275.4

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN COMPLIANCE WITH RULE 17.1(a) OR (b)

Der Präsident des Europäischen Patentamts;
Im Auftrag

For the President of the European Patent Office

Le Président de l'Office européen des brevets
p.o.

R C van Dijk

Anmeldung Nr:
Application no.: 02257275.4
Demande no:

Anmeldetag:
Date of filing: 18.10.02
Date de dépôt:

Anmelder/Applicant(s)/Demandeur(s):

Koninklijke Philips Electronics N.V.
Groenewoudseweg 1
5621 BA Eindhoven
PAYS-BAS

Bezeichnung der Erfindung/Title of the invention/Titre de l'invention:
(Falls die Bezeichnung der Erfindung nicht angegeben ist, siehe Beschreibung.
If no title is shown please refer to the description.
Si aucun titre n'est indiqué se referer à la description.)

Method, system and signal for metadata and CRID protection in TV-Anytime

In Anspruch genommene Priorität(en) / Priority(ies) claimed /Priorité(s) revendiquée(s)
Staat/Tag/Aktenzeichen/State/Date/File no./Pays/Date/Numéro de dépôt:

Internationale Patentklassifikation/International Patent Classification/
Classification internationale des brevets:

H04N7/24

Am Anmeldetag benannte Vertragstaaten/Contracting states designated at date of filing/Etats contractants désignées lors du dépôt:

AT BE BG CH CY CZ DE DK EE ES FI FR GB GR IE IT LI LU MC NL PT SE SK TR

Method, system, and signal for metadata and CRID protection in TV-Anytime

As the number of channels available to television viewers has increased, along with the diversity of the programming content available on such channels, it has become increasingly challenging for television viewers to identify television programs of interest. Historically, television viewers identify television programs of interest by analyzing printed television program guides. As the number of television programs has increased, it has become increasingly difficult to effectively identify desirable television programs using such printed guides.

More recently, television program guides have become available in electronic format, often referred to as electronic program guides (EPGs). Like printed television program guides, EPGs present overviews of the available content, which can be browsed by the user. The general term content typically comprises things like music, songs, movies, television programs, pictures and the likes, but can also refer to individual scenes, MPEG-4 objects, and so on.

The EPG compiles the overview from metadata that accompanies the individual content items. Metadata for content items is available from a variety of sources. Metadata can be included with a broadcast stream, e.g. as MPEG-2 tables, or downloaded from external databases. For example, a television receiver or Personal Digital Recorder may be provided with an Internet connection, which allows the device to access metadata made available over the World Wide Web.

This metadata generally comprises information such as title, artist, genre and so on, and may also contain a unique content reference identifier (CRID), sometimes also called a content reference identifier. Using the CRID, each individual content item can be uniquely identified. Further, using the CRID further information can be retrieved from a database. For example, a user can select a content item which he wishes to see from the EPG, even though the time and place of broadcast are not yet known. Using the CRID, the system can then retrieve the time and place of broadcast of the content item when this information becomes available.

The CRID is not restricted to broadcast transmissions of content. It could also refer to a location on the Internet, or to any other source. The purpose of content resolution is to allow acquisition of a specific instance of a specific item of content. For example a user may want to record an episode of a television series, but he does not necessarily know when and where that episode will become available. He can then use his personal digital recorder (PDR) or similar device to enter a reference to the episode or series by means of the CRID. Note that a CRID may refer to an entire series or to an individual episode thereof.

Having received a CRID for a content item, the PDR tries to obtain the location of the content item. This information is called a locator and it contains the date, time and channel on which the content item will be broadcast. The user however does not need to be aware of this. Once the PDR has obtained the locator of the content item, the PDR waits for the specified date and time and then records the episode as it is broadcast on the specified channel. Of course, if the locator indicates a location on the Internet or the like, the PDR can simply retrieve the content from the indicated location as soon as it becomes available.

The TV-Anytime standardization body provides a standardized Content Reference ID. See TV-Anytime Forum, www.tv-anytime.org. Specification Series: S-4, on Content Referencing (Normative), Document SP004V11, 14 April 2001.

The syntax of the CRID as used by TV-Anytime is as follows:

CRID://<authority>/<data>

The <authority> field indicates the body that created the CRID. An authority

will also provide the ability for the CRID to be resolved into locators or other CRIDs. A locator is the name for locations in time and space of content. The <data> field is a free format string that is compliant with the definition of Uniform Resource Identifiers (URIs) as given in RFC 2396. This string should be meaningful to the authority given by the <authority> field.

The CRID is used for location resolution, which can be defined as the process of translating a CRID into other CRID(s) or locators. For instance, a CRID for an entire TV series could be translated into a series of CRIDs for the individual episodes of that series. Location resolution may be done in the recording device (typically a Personal Digital Recorder or PDR) or remotely. A resolution provider does location resolution. Resolution providers use resolving authority records (RARs) to be identified and located. A RAR includes at least an <authority> field, corresponding to a body that creates CRIDs.

A RAR also contains a URL and the resolution provider name. The URL points to the location where resolution information can be found. The resolution provider name contains the name of the body that is providing location resolution. These RARs are made available to PDRs.

Fig. 1 schematically illustrates the process of content resolution. A Personal Digital Recorder or PDR is instructed to record a content item identified by a Content Reference Identifier CRID. Instructing the PDR to record a content item, or in other words scheduling that content item for recording can be done in a variety of ways. A presently common way is that the user manually indicates, e.g. by selecting the content item in the EPG, that the content item is to be recorded. It will be readily understood that part or all of the functionality ascribed to the PDR below could also be incorporated into one or more other devices, such as television receivers, set-top boxes or personal computers.

The PDR, or another device to which the PDR is connected, may be equipped to determine kinds of content items that the consumer may be interested in. This is known as user profiling or recommender systems. By keeping track of content items which the consumer views, and employing an implicit and/or explicit rating system for such content items, it becomes possible to predict with varying degrees of accuracy which other content items the consumer may be interested in. It then becomes possible to automatically record content items which are likely to be of interest to the consumer. Such content items could then be recorded by the PDR. Many techniques for user profiling are known in the art. When the PDR determines, using user profiling, that a particular content item may be of interest, it schedules the content item for recording.

The CRID for the content item is used to facilitate automatic recording of the content item. The CRID could be entered manually by the user, or be the result of selecting a content item through an Electronic Program Guide. This second option assumes that the CRID is somehow provided to the PDR together with other metadata used in the EPG. Alternatively, if the CRID is not known by the user or by the PDR, the user could perform a search using for example the title of the content item in a metadata database, and select the desired content item from the search results. The CRID is then supplied to the PDR by the search engine.

There are many other ways to provide the CRID to the PDR. For example, a trailer or preview for a movie could be broadcast with the CRID embedded in the content of the commercial in some way (e.g. a watermark). The user could then press a button on his remote control, television or PDR. The PDR or television then extracts the CRID from the content.

Once the CRID for the content item is known, the PDR tries to obtain locator

information for the content item, using the CRID as input. This locator information is not necessarily always available. For example, the CRID may refer to a movie that has only recently been released in movie theaters. This movie is not likely to be broadcast on television in the near future, so it cannot be scheduled using EPG information. In such a case, the PDR should regularly try to obtain the locator, as the locator may become available later (e.g. a year later, when the movie is going to be broadcast on TV). The CRID could also refer to a TV series, which is then resolved into a number of CRIDs for individual episodes of that series. It is possible that no locator information is available for some episodes. Here the PDR should also regularly retry to obtain the locator(s) for those episodes.

The process of translating a CRID into other CRIDs or locators is known in TV-Anytime as location resolution. Location resolution involves mapping a location-independent content reference (the CRID) to its location in time (e.g. scheduled transmission time in a broadcast system) and space (e.g. TV channel, IP address). As explained above, these locations in time and space are referred to as "locators." The process of location resolution may happen inside the PDR or by using a physically remote server, such as a server on the Internet.

To the PDR, the CRID essentially contains opaque information, which it cannot resolve to a location without external assistance. A Resolution Provider (RP) which provides locator information for CRIDs is provided to solve this problem. Usually multiple RPs are available, and the PDR must know which RP to use for a particular CRID. Often, this is the same body that created the CRID. The name of the authority is present in the CRID in the <authority> field, as explained above. This name is present in the form of a registered Internet domain name. It is possible for an RA to be found on the Internet using the domain name resolution process specified in the TV-Anytime specification SP004.

Each RA will require one or more Resolving Authority Records (RAR) to exist in the PDR for location resolution to take place. Each resolving authority record will need to be placed inside some sort of transport specific container which allows the PDR to know that this is a RAR. In the case of multiple records for the same authority, the PDR can choose to just use one of them, or try them all in turn. The Resolving Authority Record (RAR) contains the information that identifies the RAs where content reference resolution information can be found.

Using the RAR, the PDR determines which RP to use to resolve a particular CRID. The PDR then submits a request for a location accompanied by a CRID to the Resolution Provider in question. In response to this request, the Resolution Provider returns the locator information (assuming this information is available in that RP, of course). The PDR can then access the content source and obtain the content item. A content item may have more than one locator, for example if it is broadcast multiple times or available from multiple providers. The PDR may then choose which locator to use, or prompt the user to make a selection.

Once the locator information has been obtained, the PDR waits for the specified date and time and then records the episode as it is broadcast on the specified channel. Of course, if the locator indicates a location on the Internet or the like, the PDR can simply retrieve the content from the indicated location as soon as it becomes available.

Content items for which locator information is available can be recorded by the PDR at the appropriate moment. To this end, the PDR may comprise local storage such as a sufficiently large hard disk, and/or a device such as a DVD+RW writer. The storage on which content items are stored needs not be local to the PDR, but may also be an external device such as a hard disk or a file server connected to

the PDR via a home network. Once the content items have been recorded, they can be played back at any time until they have been erased.

TV-Anytime information and services [2][3][4] are valuable so protection of this information is important. When considering the type of protection that is needed, first the situations that are to be prevented should be identified.

The first example in which protection is needed is the case where TV-Anytime data and services are provided as a service. In this case, one wants to prevent unauthorised parties to access to this service. Only authorised parties should be allowed to access the data. In other words, the service and/or data should be placed under access control.

The other example regards the issue of source authentication and spoofing; the integrity of the data is to be protected. When TVA data is received from a source, the receiver may want to check if the data is indeed coming from the expected source and hasn't been changed by a third party.

There is an incentive for a third party to try this. If a third party can change the metadata or CRID table, it can make the PDR record other information then was intended including commercials, trailers or just other content.

This is also very annoying for a user and may lower the trust the user has in the system. This brings us to another level of authentication. The PDR may want to check whether the content came from a trusted source. If the data can be authenticated to originate from one source even when it is distributed using different channels, the PDR can use this to make a choice when confronted with multiple sources of the same content. An example of this is when the data of a certain BBC show can be authenticated as being generated by the BBC, this raises the likelihood that this information is correct.

From this discussion, we can conclude that there is an incentive for service providers and box manufacturers to use access control and integrity checking mechanisms. The approach towards access control and protecting the data integrity of TV-Anytime data will also be handled.

[1] TV-Anytime document WD659, *Final report of RMP WG*, RMP working group, September 2002

[2] TV-Anytime document WD647/SP003v1.3 Part A, *Specification series S-3 on Metadata: Part A Metadata Schemas*, Provisional Specification, Version 1.3, 27 September 2002.

[3] TV-Anytime document WD647/SP003v1.3 Part B, *Specification series S-3 on Metadata: Part B System Aspects in a Unidirectional Environment*, Working Draft Version 1.3, 2 August 2002

[4] TV-Anytime document SP004v1.2, *Specification series S-4 on Content Referencing*, Version 1.2, Final Specification, 28 June 2002.

[5] Provisional TV-Anytime document SP006v0.1, *Specification series S-6 on Delivery of Metadata over a Bidirectional* Network, 10 October 2002

[6] ISO/IEC 13818-1:1996(E), *Information technology – Generic coding of moving pictures and associated audio information: Systems*, First Edition, 1996-04-15.

[7] ISO/IEC 13818-6:1998, *Information technology -Generic coding of moving pictures and associated audio information: Extensions for Digital Storage Media Command and Control*, 1998.

[8] ETSI TS 102 812 V1.1.1 (2001-11), Digital Video Broadcasting (DVB): Multimedia Home Platform (MHP) Specification 1.1, 28 June 2002.

[9] RFC3275, *(Extensible Markup Language) XML-Signature Syntax and*

Processing.
[10]Applied Cryptography Second Edition: protocols, algorithms, and source code in C, Bruce Schneier, Wiley, 1996.
[11]RFC2396, *Uniform Resource Identifiers (URI): Generic Syntax.*

If the PDR operates in accordance with a Digital Rights Management system, then a content item may be erased when the rights associated with the content item require such erasure. Also, some content items may not come with a right to record the item at all, or with a right that permits viewing only for a limited amount of time, or for a limited number of times. The PDR should then erase the content item when the limit is exceeded, or refuse further access to the content until further rights are obtained that permit further access.

Using the above approach, anyone knowing the location of content could act as a resolution provider. Content and service providers, however, may desire that only authorized resolution providers perform content resolution for their content, for example to be able to protect their reputation. On the other hand, for consumers and PDRs it is important to be able to rely on/trust the CRID authority and resolution provider, so that they can obtain the correct content.

So, it is desirable to enhance the above approach so that at least one aspect of the CRID and/or other metadat and/or the resolution process can be protected. This protection preferably involves data origin authentication or integrity protection, but can also involve protection against unauthorized access, or maintenance of confidentiality.

Access control can be used in order to make sure that only authorised clients can access the services. Of course, it should be impossible (or very difficult) for unauthorised clients to access the data. Whether a client is authorised is determined by the service provider. Furthermore, different models for accessing the content can be introduced. Examples of such models could be that there are several different levels of service that a client can buy. The basic model will just give information regarding the content of a few channels over a limited period of time. More advanced models will provide access to a larger range of services and span a longer time period.

The models described in the previous paragraph are very similar to the models used by pay-TV operators. Only authorised users (subscribers) are allowed access to the content. Furthermore, the level of access you get is dependent on your subscription. Similar systems exist on the Internet, where they are called DRM systems.

Although the level of standardisation is different in both cases, the model shown in Fig 2. for secure delivery of TV-Anytime content to a client applies to both.

The content is received in the client box. During transport, the content is encrypted. Before the content can be accessed, the content has to be decrypted. This process is controlled by the DRM or CA system.

The TV-Anytime specification distinguishes between two different distribution media: unidirectional and bidirectional. In the unidirectional situation, TV-Anytime data is another stream in the broadcast stream with the normal signalling in place. In this case the access to this stream can be protected using traditional conditional access systems. This would mean that the stream broadcasted while scrambled. Using the normal signalling methods defined for the transport mechanism, the conditional

access system is identified and the messages carrying the conditional access information related to this stream are indicated. Most digital broadcast systems use the MPEG-2 transport stream format [6].

In the bidirectional case, a point to point connection is made between client and server. This process is described in [4]. In this case the DRM system will open a secure channel to the service provider and tunnel the communication described in [4] through this channel. In this way it will ensure that only authorised TV-Anytime clients can access the content.

Although existing CRC mechanisms in the broadcast system will deal with transmission errors, it remains wishful to detect intentional changes and to authenticate that the information was generated by the claimed source.
As is apparent in the previous discussion, applying conditional access upon TV-Anytime services can be achieved using protection methods.

It is described how TV-Anytime data integrity can be protected. Any TV-Anytime data integrity approach is closely linked to the way the data is delivered. Furthermore, the analysis provided indicates that two different levels of data integrity are needed.

The first level of integrity relates to the service provider that delivers the metadata. The intention is to validate whether the data has not been changed during transport between resolution provider and the client.

The second level of integrity relates to the validation of the actual source of the information. The source of the TV-Anytime data is not always the creator of the data. The source could be a service provider gathering and grouping information from different sources. It could be useful to check who created to data and whether the data has been changed. In this case, the data that is received will hold parts provided by different sources.

It is an object to protect the integrity of TV-Anytime data during delivery. In the case the data is also protected by a conditional access or DRM system (section 3), delivery integrity protection is easy. When the TV-Anytime data is delivered under control of a conditional access or DRM system, these systems ensure that only authenticated clients can access the data. As this involves encryption of the data during delivery, this process also authenticates the source of the information. When the content is not protected by such systems, other mechanisms can be used. The standard cryptographic approach to protection of data integrity is to sign the data use cryptographic techniques [9].

In a unidirectional broadcast scenario, a reasonable argument can be made that it is sufficiently difficult to change the broadcast stream. Although this is a valid argument, in some situations additional protection may be needed, by adding mechanisms to protect the integrity are part of the delivery system, such as a system to sign files with the data.

In the situation that such mechanisms are not available or a different mechanism is need, the proposal indicated in this chapter can be used.

When studying the TV-Anytime specifications [2], [3], [4] & [5], the following types of data are identified: metadata and CRIDs. Furthermore, as TV-Anytime defines two different delivery mechanisms (unidirectional [3] and bi-directional [5]), care has to be taken not to propose any mechanism that would break these existing specifications.

All TVA metadata is provided as TVA fragments. In TVA, according to [2] a TVA fragment is "a self contained atomic portion of the metadata". In this document, we assume that the smallest TVA metadata element that can be signed is a fragment.

In order to sign a fragment or a set of fragments several issues need to be considered. The method should allow for different forms of encoding (BiM, text). Furthermore, the technology should preferably be compatible with the unidirectional as well as the bi-directional distribution system. Furthermore, the level of change that adding signatures will impose upon the existing metadata specification should preferably be limited.

During distribution, when metadata changes hands, more than one party may want to apply their signature to the same fragment, so the system should preferably support such this. Furthermore, it is likely that for efficiency reasons it is required to sign a set of metadata fragments instead of individual fragments. Concluding, the system supports signatures over single or multiple fragments.

When considering these requirements two approaches can be considered:

1. Add signatures and signature information to the fragment.
2. Sign references and provide separate signature file

As solution one will not allow the same signature to cover more than one fragment, we will target a system in which signatures will be provided separately and a reference will indicate which elements are signed.

As all TVA metadata is expressed in XML, a transport neutral way of expressing signatures that allows the signatures to be carried in the same data structure would be to include the signatures in the TVA schema. As TV-Anytime metadata is expressed in XML an obvious choice would be xmldsig [9].

The way to define the fragments that need to be signed can be approached by defining a transform function [9] that removes some or all elements from the metadata that are not considered for this signature. Another approach is to label each individual fragment or set of fragments and sign using references. The last approach has the advantage that, when properly chosen, the reference would provide a link from the signature file to the fragment. Furthermore, the label provides a link between the fragment(s) and the data containing the signature.

In order to protect the integrity of the references, they might either implicitly or explicitly be included in the data to be signed.

More elaborate search options could be provided by adding signature index files. Such index file would than link labels to the appropriate signature files.

As is explained in [7] & [8], digital signatures are implemented by calculating a hash over the content and signing the hash using public key cryptography. This requires the client to know the public key of the party the applied the signatures. Typical this information is carried in signed certificates. So in order to check the signature, in addition to the signatures data, also the certificates of the parties providing signatures are required. We suggest to add an additional element to TVAMain; certificates.

According to [3] the following fragments have been defined by TV-Anytime.

- TVAMain
  - ClassificationTable
    - CSAlias
    - ClassificationScheme
  - ProgramDescription
    - ProgramInformationTable
      - ProgramInformation
    - GroupInformationTable
      - GroupInformation

- ProgramLocationTable
  - BroadcastEvent
  - Schedule
- ServiceInformationTable
  - ServiceInformation
- CreditsInformationTable
  - PersonName
  - OrganisationName
- ProgramReviewTable
  - ProgramReviews
- SegmentInformationTable
  - SegmentInformation
  - SegmentGroupInformation
- OnDemandProgramLocation

This section will define the label that is used to uniquely identify a TV-Anytime fragment in order to link the fragment to the signature. This is done by providing an optional field that is added to each TV-Anytime fragment. When present it is a unique identification of that fragment instance within this instance of metadata. The label should allow for easy tracing of the fragment within the metadata. This is required in order to find the different fragments that are needed to calculate a signature.

Within the TV-Anytime specification, a field called TVAID is used. According to the metadata specification [2] TVAIDs are used to "indicate uniqueness within a metadata description" [2]. Although they seem to match the requirement for an identifier, they're only unique for a particular type of TVAID. e.g. a serviceID and segmentID could be the same within a particular metadata description. This could be enough if the reference used in the signature indicated the context (e.g. service or segment).

In order to support signatures, all fragments have an optional or compulsory fragment identification. The TVAID could be used if all fragments have one (or one is added) and it is determined that using the TVAID a unique reference to the fragment can be made within this instance of the TVA metadata.

Another solution could be that a special TVA signature identifier is added to all fragments as an optional field. Either the TVAID or a new identifier is defined for this purpose. When the TVAID is used, and it is added to all fragments, the signature defined in this section could be replaced by the TVAID.

An example identifier used for signatures is defined as

```
<simpleType name="TVASignatureIdType">
  <restriction base="string">
    <whiteSpace value="collapse"/>
  </restriction>
</simpleType>
```

Name	Definition
TVASignatureIdType	A simpleType used to add an optional identifier to each TVA fragment that uniquely identifies this fragment among

other fragments of the same type within this instance of metadata.

In order to be able to reference each fragment (or set of fragments), an example of a format for all TV-Anytime fragments could be

```
<attribute name="TVASignatureId"
    type=" TVASignatureIdType " use="optional"/>
```

In order to ensure that the identifier is unique among fragments of the same type within this instance of metadata it is suggested to start the identifier with the DNS name of the organization responsible of generating the fragment. So the TVASignatureId of a fragment published by company MyCompany could look like:

```
<TVASignatureId>MyCompany.com;1231bahdga7219
</TVASignatureId>
```

This would also allow the client to detect what organization published the data.

In xmldsig [9], references can be used to indicate the elements grouped to calculate a signature. The reference is implemented as an URI [11]. So in order to indicate which fragments are used to calculate a signature, the URI to refer to the fragments needs to be defined.

Although the TVASignatureId identifies a fragment, it does not define where this fragment can be found within the total TVAMain. In order to facilitate the searching of the correct fragment within the metadata, the URI should preferably also indicate the location.

A way of doing this would be to indicate the path through the metadata that has to be taken in order to locate the fragment (see Appendix A).

So the definition of the fragment URI (formatted according to [11]) is:

tva://<path>/<TVASignatureId>

path, the path from the start of the metadata towards the fragment.

TVAID, the identifier of the fragment

Some examples:

tva://TVAMain/aap.org;132423

tva://TVAMain/ClassificationTable/CSAlias/publisher.com;122314

[illegible]/TVAMain/ProgramDescription/ProgramLocationTable/Schedule/metwt.org;3[illegible]84

As can be seen it is also possible to sign TVAMain. In this case, all of TVAMain without the certificate and signature parts should be considered. The TVASignatureId is used in URIs to refer to a fragment, as such the identifier should be compatible with the formatting restrictions placed upon URIs [11]. Furthermore, in order to ease the parsing of the URI no slashes ("/") may be used in the TVASignatureId.

The system described in previous sections requires that the signatures are

distributed and access within the normal distribution system as is indicated by TV-Anytime. This can be done in two ways, one could expand the TVAMain object so it will include the signature information.

Another approach would be to define a wrapper that includes the TVAMain and possibly some other elements that need signing. In this way, this specification would not change the current metadata specification and it would also allow to include other TV-Anytime documents (e.g. ContentReferencingTable and ResolvingAuthorityRecordTable). Seeing these advantages, a wrapper format has been defined (TVASignatureWrapper).

This table will provide a grouping between the data that is signed and the list of signatures; the TVASignatureTable

```
<element name="TVASignatureWrapper"
      type="tva:TVASignatureWrapperType"/>

<complexType name="TVASignatureWrapperType">
  <attribute name="TVAMain"
     type="tva:TVAMainType" use="required"/>
  <attribute name=" ContentReferencingTable"
     type="tva: ContentReferencingTableType" use="required"/>
  <attribute name=" ResolvingAuthorityRecordTable"
     type="tva: ResolvingAuthorityRecordTableType" use="required"/>

  <attribute name="SignatureTable"
     type="tva:TVASignatureTableType " use="required"/>

  <attribute name="KeyInfoTable"
     type="tva:KeyInfoTableType" use="required"/>

  <attribute name="version" type="integer" use="optional"/>
  <attribute ref="xml:lang" default="en" use="optional"/>
  <attribute name="publisher" type="string" use="optional"/>
  <attribute name="publicationTime" type="dateTime" use="optional"/>
  <attribute name="rightsOwner" type="string" use="optional"/>
  <attribute name="copyrightNotice" type="string" use="optional"/>
</complexType>
```

Name	Definition
TVASignatureWrapper	A complextype hold TV-Anytime data and the accompanying signatures.
TVAMain	A TVAMain instance holding fragments that have been signing by signatures in the SignatureList
ContentReferencingTable	A ContentReferencingTable that has been signing by signatures in the SignatureList
ResolvingAuthorityRecordTable	A ResolvingAuthorityRecordTable that has been signing by signatures in the SignatureList
SignatureTable	The list with signatures of data elements (see text).

KeyInfoTable	The list with KeyInfoWrapper objects (see text).
Version	Specified the version of the description
Xml:lang	Specifies the language of the description. Default is 'English.'
Publisher	Specifies the name of the publisher of the description
PublicationTime	Specifies the time the metadata description was published.
RightsOwner	Specifies the entity that holds the rights to the description
CopyrightNotice	Specifies the copyright information for the description document.

In this table, also the option is given to include the ContentReferencingTable and ResolvingAuthorityRecordTable in this table. As they can only occur once, no "fragment identifier" is needed in the table as well for definition of the URI.

```
<complexType name="TVASignatureTableType">
  <sequence>
    <element name="Signature"
      type="ds:SignatureType" minOccurs="0"
      maxOccurs="unbounded"/>
  </sequence>
</complexType>
```

Name	Definition
SignatureTableType	A complextype that contains a list of signatures
SignatureList	A list of signature information elements as specified in text

As can be seen, 0 or more signatures can be present. This brings us to what information is available. In the ideal world, all signatures available for the data indicated in TVASignatureWrapper are included and all fragments that are indicated in the different signatures are present.
In the bi-directional delivery system, this could be different as only the requested fragments are present. As these issues are very delivery system dependent, they should be handled in future versions of the respective specifications.

In order to check the signatures, a public key is needed. Distribution of this key can be done in several ways. The can be hard coded in the devices but this would raise problems if new keys are used or when current keys are compromised. The most common way of distribution of the keys is by incorporating them into a so-called certificate-chains [10]. TVASignature allows the inclusion of one or more ds:KeyInfo objects in order to support the carriage of such certificates within the TVASignature wrapper.

A complextype indicating a list of KeyInfo objects with accompanying identifiers.

```
<complexType name="KeyInfoWrapperType"
  <attribute name="Identifier" type="string" use="required"/>
  <attribute name="KeyInfo" type="ds:KeyInfoType" use="required"/>
</complexType>

<complexType name="KeyInfoTableType"
  <sequence>
    <element name="KeyInfoWrapper"
      type=" KeyInfoWrapperType " minOccurs="0"
      maxOccurs="unbounded"/>
  </sequence>
</complexType>
```

Name	Definition
KeyInfoWrapperType	A complextype that contains the signatures present in this TVAMain
Identifier	A unique identifier of this KeyInfo object.
KeyInfo	The key information (see text).
KeyInfoListTableType	A list of KeyInfoWrappers.
KeyInfoWrapper	A KeyInfo with identification.

In order to be able to refer from a signature to KeyInfo elements in the KeyInfoWrapperTable from the Signatures, the reference URI needs to be defined. This URI is similar to the one defined in section 4.2.2.
So the definition of the URI (formatted according to [11]) is:
tva://KeyInfoListTable/<Identifier>
Identifier, the identifier indicated in the KeyInfoWrapperType.

Some examples:
tva:// KeyInfoListTable /132423
tva:// KeyInfoListTable/435432h
tva:// KeyInfoListTable /MyKeyInfo

This allows the inclusion of certificates but also of other options of communicating KeyInfo objects and indicates how they are linked to signatures.
We state how TV-Anytime signatures are made, the process and what part of xmldsig are used (and not used) in TV-Anytime.
It can be specified, for example, that DSA is optional and RSA required.
As is explained in the xmldsig specification, text can be coded in many ways. In order to calculate the signature, one defined representation of the document has to be defined. This process is called cannolization.
Within TV-Anytime, BiM is used as a binary codex for the binary encoding of TV-Anytime data. When BiM encoding is used, BiM should be indicated as the cannolization function. This would allow the client to use the BiM encoded files to calculate the signature values without the need of extracting the data first.
Signatures can also be used on the different tables. Signing individual CRIDs is more difficult.
In an embodiment of the invention, digital signatures are used to sign the content of the CRID. Only properly signed CRIDs will be accepted by the PDRs.

Such CRIDs can be trusted to originate from a trustworthy authority. It does not protect against incorrect resolution of the CRID. Having correctly verified the signature, the PDR can assume that the CRID is authentic. If the signature is not verified as correct, the PDR should refuse to obtain a locator for the content using the CRID. Thus, content and service providers can be sure that PDRs will only obtain content using authentic CRIDs. A further advantage of this aspect is that this allows a PDR to detect a malformed or corrupted CRID, since such a CRID would also have an invalid digital signature.

Signing individual CRIDs preferably has to be done without changing the CRID format. Furthermore, the amount of information is small, making the protection weaker.

A way to add signatures to individual CRIDs is by adding them to the end of the CRID. In this way, the signature would be part of the data part of the CRID and will not harm normal behaviour.

As the amount of information that can be added to a CRID is limited, only the core can be specified. Furthermore, due to the size of the CRID, no hashing is needed and the signature can be directly calculated using a PKI algorithm.

The CRID is redefined using the following syntax:

The syntax of a signed CRID is:

CRID://<*authority*>/<*data*>&<*signatureAuthority*>:<*signature*>

<authority> Uses the *TV-Anytime* authority naming rules given in section 7 of SP002 to assure uniqueness.

<data> is a free format string that is Uniform Resource Identifier (URI) compliant, and is meaningful to the authority given by the <authority> field. The <data> portion of the CRID is case insensitive.

<signatureAuthority> Uses the *TV-Anytime* authority naming rules given in section 7 of SP002 to assure uniqueness. The signatureAuthority indicates the party that defined the algorithm and manner of calculating the signature.

<signature> The signature value of this CRID calculated as defined by the signatureAuthority.

More than one signature can be applied by resigning the signed CRID. Some or all of the previous signatures can be included in the competition of a new signature. This could be indicated using another additional field, for example separated by one of the other (reserved) characters.

Some examples of signed CRIDS are:

CRID://comp.com/3874y32&comp.com:32843829174

CRID://broadcast.com/1.4.5&sign.com:7asd76ad7

As a variation of this method, it is possible to use a different URL type to represent a signed CRID. An example of this variation is:

SCRID://comp.com/3874y32&comp.com:32843829174

Different orders and different characters could be used to comprise the new signed CRID.

Also, a restriction could be added that indicated markers may not be used in the data part ("&" and ":").

The measures used in the above embodiments can be used individually, but these measures could also be combined to provide for better protection, or for protection against multiple threats.

It should be noted that the above-mentioned embodiments illustrate rather than limit the invention, and that those skilled in the art will be able to design many alternative embodiments without departing from the scope of the appended claims.

In the claims, any reference signs placed between parentheses shall not be construed as limiting the claim. The word "comprising" does not exclude the presence of elements or steps other than those listed in a claim. The word "a" or "an" preceding an element does not exclude the presence of a plurality of such elements. The invention can be implemented by means of hardware comprising several distinct elements, and by means of a suitably programmed computer.

In the device claim enumerating several means, several of these means can be embodied by one and the same item of hardware. The mere fact that certain measures are recited in mutually different dependent claims does not indicate that a combination of these measures cannot be used to advantage.

Of course, the techniques above can also be used outside the scope of TV anytime.

CLAIMS:

1. A method for protecting the integrity of metadata in a content stream, substantially as described in this document.

2. The method of claim 1, in which the protection of metadata is performed using a signature

3. The method of claim 2, in which the sections which are protected using a signature are identified with a unique identifier

4. The method of claim 2, in which the metadata is processed into a different format before the signature is computed

5. The method of claim 1,in which the signatures are to be carried in the same data structure as said metadata

6. The method of claim 1, in which a transform function is used to select at least one section of the metadata that has been signed

7. The method of claim 3, in which the unique identifier contains at least one start field and one end field for the identified metadata

8. The method of claim 1,in which certificates are used to verify the signature

9. A system that handles potentially protected metadata, further characterized in that it implements signing, and encryption, decryption, and verification of protected metadata, substantially as described in this document.

10. A signal that is carrying metadata, including optional additional labeling and signatures to protect said metadata.

11. A method of providing a content reference identifier CRID, characterized by applying a measure to the CRID, to a locator obtained by resolving the CRID, and/or to a resolution authority record (RAR) used in the process of resolving the CRID so as to obtain said locator, to provide for authentication of at least one aspect thereof.

12. The method of claim 1, whereby the measure comprises computing a digital signature over at least part of the contents of the CRID, the locator and/or the RAR.

ABSTRACT:

This invention concerns a method, system for the protection of the integrity of TV anytime metadata, and a signal carrying such protected information accordingly. Protection is obtained by applying a signature and certification approach. Optionally, an additional step of cannolization or a transform function is used. Metadata can be labeled with a unique identifier so they can be referenced and separately signed individually or as a set by several different parties.

Fig. 1
Fig. 2

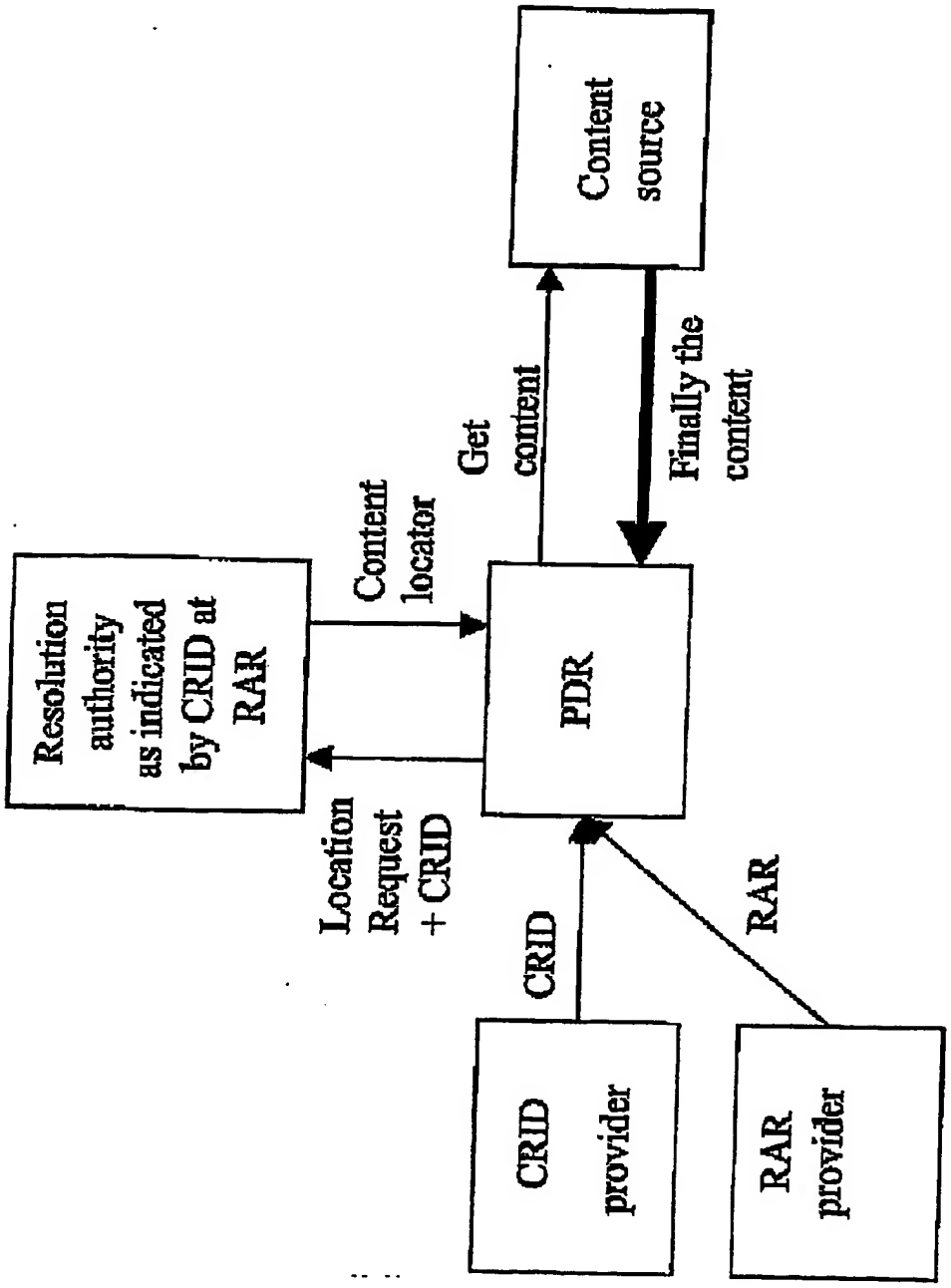

Content source
Get content
Finally the content
Content locator
Resolution authority as indicated by CRID at RAR
PDR
Location Request + CRID
CRID
RAR
CRID provider
RAR provider

Fig. 1

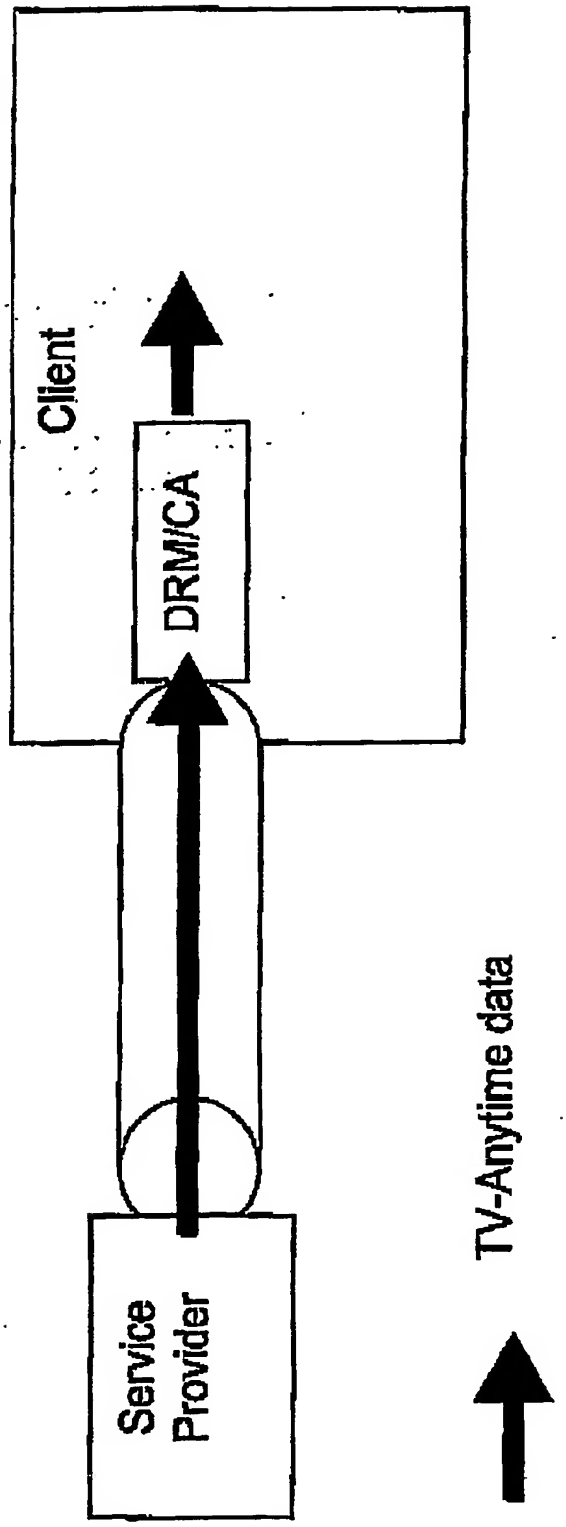
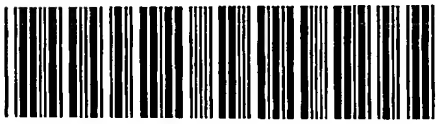


Fig. 2

PCT Application
IB0304608



0050197 :18-Oct-02 11:0